Downloaded from orbit.dtu.dk on: May 05, 2023

DTU Library

Further Generalisations of Twisted Gabidulin Codes

Puchinger, Sven ; Rosenkilde, Johan Sebastian Heesemann; Sheekey, John

Published in:
Proceedings of International Workshop on Coding and Cryptography 2017

Publication date:
2017

Document Version
Peer reviewed version

Link back to DTU Orbit

Citation (APA):
Puchinger, S., Rosenkilde, J. S. H., & Sheekey, J. (2017). Further Generalisations of Twisted Gabidulin Codes. In *Proceedings of International Workshop on Coding and Cryptography 2017*

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Further Generalisations of Twisted Gabidulin Codes

Sven Puchinger[1], Johan Rosenkilde né Nielsen[2], and John Sheekey[3]

[1] Institute of Communications Engineering, Ulm University, Ulm, Germany
sven.puchinger@uni-ulm.de
[2] Department of Applied Mathematics & Computer Science, Technical University of Denmark, Lyngby, Denmark
jsrn@jsrn.dk
[3] School of Mathematics and Statistics, University College Dublin, Dublin, Ireland.
john.sheekey@ucd.ie

Abstract We present a new family of maximum rank distance (MRD) codes. The new class contains codes that are neither equivalent to a generalised Gabidulin nor to a twisted Gabidulin code, the only two known general constructions of linear MRD codes.

1 Introduction

Rank-metric codes are sets of matrices, where the distance of two elements is measured with respect to the rank metric, i.e., the rank of their difference. These codes have found many applications, such as random linear network coding [25], MIMO communication [7], cryptography [8], and distributed storage [24]. A rank-metric code is called a maximum rank distance (MRD) code if its minimum rank distance is maximal for the given parameters.

The first known class of MRD codes are Gabidulin codes, which were independently introduced in [5,6,21]. They are evaluation codes of skew polynomials [17] that are defined using the Frobenius automorphism $\cdot^q$ of a finite field extension $\mathbb{F}_{q^m}/\mathbb{F}_q$. Gabidulin codes were generalised in [1,12,22] using other automorphisms.

The first families of MRD codes that are not equivalent to a generalised Gabidulin code were independently introduced in [23] (twisted Gabidulin codes) and [18], where the latter is a special case of the first. Similar to Gabidulin codes, twisted Gabidulin codes were generalised using different automorphisms in [23, Remark 9] and [13]. Other constructions, leading to non-linear codes or codes with restricted parameters, can be found in [4, 11, 19].

Recently, the idea of "twisting" was transferred to Reed–Solomon codes, the Hamming metric analogue of Gabidulin codes [2]. This transfer resulted in new generalisations of the "twisting" idea and tools for the analysis of the new codes.

In this paper, we introduce a new class of rank-metric codes using ideas from [23] and [2] (cf. Section 3). A sufficient condition for the new codes to be MRD is derived in Section 4. In Section 5, we show that the new family contains MRD codes that are not equivalent to generalised Gabidulin or to the

twisted Gabidulin codes in [23]. Finally, we briefly discuss a possible application to cryptography in Section 6 and conclude the paper in Section 7.

2 Preliminaries

The following are well-known facts on skew polynomials over finite fields, see e.g. [14,17]. Let $\mathbb{F}_{q^m}/\mathbb{F}_q$ be a finite extension of a finite field and $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ be a generator of the Galois group of the extension, i.e., $\sigma = (\cdot)^{q^i}$, where $\gcd(i,m) = 1$. The skew polynomial ring $\mathbb{F}_{q^m}[x;\sigma]$ is the set of formal polynomial expressions $a = \sum_i a_i x^i$, where $a_i \in \mathbb{F}_{q^m}$, with ordinary component-wise addition $+$ and the following multiplication rule:

$$\left(\sum_i a_i x^i\right) \cdot \left(\sum_i b_i x^i\right) = \sum_i \left(\sum_{j=0}^{i} a_j \sigma^j\left(b_{i-j}\right)\right) x^i.$$

We define the degree of $a = \sum_i a_i x^i \in \mathbb{F}_{q^m}[x;\sigma]$ by $\deg(a) := \max\{i : a_i \neq 0\}$ (and $\deg 0 := -\infty$) and the (operator) evaluation map [3] by

$$a(\cdot) : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}, \quad \alpha \mapsto \textstyle\sum_i a_i \sigma^i(\alpha)\,.$$

Since σ is an automorphism that fixes $\mathbb{F}_q$, the evaluation map of a skew polynomial is an $\mathbb{F}_q$-linear map and its root space $\ker(a)$ is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^m}$ (seen as an m-dimensional vector space over $\mathbb{F}_q$). Since σ is a generator of $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$, we know that $\dim \ker(a) \leq \deg a$. For any subspace $\mathcal{S} \subseteq \mathbb{F}_{q^m}$, there is a unique monic polynomial $\mathcal{A}_\mathcal{S}$, the *annihilator polynomial of* $\mathcal{S}$, of minimal degree whose kernel contains $\mathcal{S}$. Its degree is $\deg \mathcal{A}_\mathcal{S} = \dim_{\mathbb{F}_q}(\mathcal{S})$.

The ring of skew polynomials is left and right Euclidean [17], so the greatest common right divisor gcrd and the right modulo operator $\bmod_{\mathrm{r}}$ are well-defined.

Definition 1. *Let $\mathcal{V}$ be a k-dimensional $\mathbb{F}_{q^m}$-linear subspace of $\subset \mathbb{F}_{q^m}[x;\sigma]$. Let $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_{q^m}$ be linearly independent over $\mathbb{F}_q$ and write $\boldsymbol{\alpha} = [\alpha_1, \ldots, \alpha_n]$. Then we define the* evaluation map *of $\boldsymbol{\alpha}$ on $\mathcal{V}$ by*

$$\mathrm{ev}_{\boldsymbol{\alpha}} : \mathcal{V} \to \mathbb{F}_{q^m}^n, \quad f \mapsto [f(\alpha_1), \ldots, f(\alpha_n)].$$

We call $\alpha_1, \ldots, \alpha_n$ the evaluation points *of $\mathrm{ev}_{\boldsymbol{\alpha}}$.*

Note that $\mathrm{ev}_{\boldsymbol{\alpha}}$ is an $\mathbb{F}_{q^m}$-linear map. Furthermore, $\ker \mathrm{ev}_{\boldsymbol{\alpha}} = \{f\mathcal{A}_{\boldsymbol{\alpha}} \mid f \in \mathbb{F}_{q^m}[x;\sigma]\} \cap \mathcal{V}$. If all elements of $\mathcal{V}$ have degree less than n, $\mathrm{ev}_{\boldsymbol{\alpha}}$ is invertible.

Definition 2. *Given $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_{q^m}$ which are linearly independent over $\mathbb{F}_q$ as well as k with $1 \leq k \leq n$ and some $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$, then the* $[n,k]$ Gabidulin code $\mathcal{C} \subset \mathbb{F}_{q^m}^n$ with defining automorphism σ and evaluation points $\boldsymbol{\alpha} = [\alpha_1, \ldots, \alpha_n]$ *is the set:*

$$\mathcal{C} = \mathrm{ev}_{\boldsymbol{\alpha}}(\langle 1, x, \ldots, x^{k-1}\rangle_{\mathbb{F}_{q^m}}) \subset \mathbb{F}_{q^m}^n\ ,$$

where x is the indeterminate of $\mathbb{F}_{q^m}[x;\sigma]$.

From the properties of $\mathrm{ev}_{\boldsymbol{\alpha}}$, a Gabidulin code is a linear code of dimension k. When $\sigma \neq (\cdot)^q$ then a Gabidulin code with defining automorphism σ is sometimes called a "generalised Gabidulin code".

For any $a = (a_1, \ldots, a_n) \in \mathbb{F}_{q^m}^n$ we define $\mathrm{rk}(a) := \dim_{\mathbb{F}_q} \langle a_1, \ldots a_n \rangle$. In other words, $\mathrm{rk}(a)$ is the rank of the $\mathbb{F}_q^{m \times n}$-matrix obtained by expanding each a_i into an $\mathbb{F}_q^m$-vector over any basis of $\mathbb{F}_{q^m}/\mathbb{F}_q$. We then endow $\mathbb{F}_{q^m}^n$ with the *rank metric over* $\mathbb{F}_q$, for $a, b \in \mathbb{F}_{q^m}^n$ we define $\mathrm{d_R}(a, b) := \mathrm{rk}(a - b)$. A "rank metric code" is simply a linear code over $\mathbb{F}_{q^m}$ whose properties are considered wrt. the rank metric. A Gabidulin code $\mathcal{C}$ attains the Singleton bound for the rank metric, that is, $\mathrm{d_R}(\mathcal{C}) = n - k + 1$. Codes attaining this bound are called Maximal Rank Distance codes, or MRD.

3 A New Construction

3.1 Idea

Gabidulin codes are MRD since any non-zero skew polynomials $f \in \mathbb{F}_{q^m}[x; \sigma]$ of degree at most $k-1$ has a space of roots of dimension at most $k-1$. Hence by evaluating f at n linearly independent elements of $\mathbb{F}_{q^m}$, the result spans a subspace of dimension at least $n - k + 1$.

The paper [23] considered skew polynomials of the form $f = f' + \eta f_0 x^k$ where $\deg f' \leq k-1$, f_0 is the constant coefficient of f', and $\eta \in \mathbb{F}_{q^m}$ is some fixed constant. He showed that by choosing η carefully, any such f will *also* have a space of roots of dimension at most $k-1$, even though f has degree k. Applying the evaluation map to this space of polynomials immediately gives an MRD code which turns out to be inequivalent to a Gabidulin code; these codes were dubbed "twisted Gabidulin codes". [23] mainly discussed $\sigma = (\cdot)^q$, but it is straightforward to use any generator $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$, see [23, Remark 9] or [13].

In this paper we consider the obvious generalisation of "twisting" in other ways than with (a multiple of) f_0 at the monomial x^k. One e.g. immediately thinks of polynomials of the form $f = f' + \eta f_h x^{k-1+t}$, where f_h is the coefficient to x^h in f' for some $h \in \{0, \ldots, k-1\}$ and $t \in \{1, \ldots, n-k\}$. "Multiple twists" is the next natural idea, e.g. $f = f' + \eta_1 f_{h_1} x^{k-1+t_1} + \eta_2 f_{h_2} x^{k-1+t_2}$. The difficulty lies in how to argue that the resulting polynomials never have a space of roots of dimension greater than $k-1$, within the space spanned by the evaluation points. The tools we develop for this are very different from those of [13, 23] but are completely analogous to those of the recent "Twisted Reed–Solomon codes" [2]. It turns out that those tools cope effortlessly with an even more general notion of twisting, where the $f_{h_1}, f_{h_2}, \ldots$ are replaced with arbitrary linear combinations of all the $f_0, \ldots, f_{k-1}$, i.e.:

$$f = \sum_{j=0}^{k-1} f_j x^j + \sum_{i=1}^{\ell} \eta_i \left(\sum_{j=0}^{k-1} \lambda_{i,j} f_j \right) x^{k-1+t_i}.$$

for fixed $\eta_1, \ldots, \eta_\ell$ and $\lambda_{i,j}$ for $i = 1, \ldots, \ell$ and $j = 0, \ldots, k-1$.

This generalization comes at the cost of shorter code lengths n since we will need to restrict the choice of evaluation points. On the other hand, our codes

are very constructive: the restrictions on choosing the evaluation points and the parameters η_i and $\lambda_{i,j}$ are simply that they belong to or avoid certain sub-fields of $\mathbb{F}_{q^m}$, and are therefore easily satisfied.

We also call our new codes "Twisted Gabidulin codes", and consider the codes of [13, 23] special twists.

3.2 Formal definition

Let $n, k, \ell \in \mathbb{N}$ be such that $k < n \leq m$ and $\ell \leq n - k$. Furthermore, let $\eta_1, \ldots, \eta_\ell \in \mathbb{F}_{q^m} \setminus \{0\}$ as well as $0 < t_1 < t_2 < \ldots < t_\ell < n - k$. For $i = 1, \ldots, \ell$, let $\lambda_i : \mathbb{F}_{q^m}^k \to \mathbb{F}_{q^m}$ be $\mathbb{F}_{q^m}$-linear maps. Write $\boldsymbol{\eta} = [\eta_1, \ldots, \eta_\ell]$; $\boldsymbol{t} = [t_1, \ldots, t_\ell]$; and $\boldsymbol{\lambda} = [\lambda_1, \ldots, \lambda_\ell]$. We define the set of $(k, \boldsymbol{t}, \boldsymbol{\lambda}, \boldsymbol{\eta})$-*twisted skew polynomials* by

$$\mathcal{V}_{k,\boldsymbol{t},\boldsymbol{\lambda},\boldsymbol{\eta}} = \left\{ f = \sum_{i=0}^{k-1} f_i x^i + \sum_{i=1}^{\ell} \eta_i \lambda_i(f_0, \ldots, f_{k-1}) x^{k-1+t_i} : f_i \in \mathbb{F}_{q^m} \right\}.$$

Definition 3. *Let $n, k, \ell, \boldsymbol{t}, \boldsymbol{\lambda}, \boldsymbol{\eta}$ be as above and $\boldsymbol{\alpha} := [\alpha_1, \ldots, \alpha_n] \in \mathbb{F}_{q^m}$ be such that $\alpha_1, \ldots, \alpha_n$ are linearly independent over $\mathbb{F}_q$. The corresponding (ℓ-)*twisted Gabidulin code *is defined by*

$$\mathcal{C}_k(\boldsymbol{\alpha}, \boldsymbol{t}, \boldsymbol{\lambda}, \boldsymbol{\eta}) := \mathrm{ev}_{\boldsymbol{\alpha}}(\mathcal{V}_{k,\boldsymbol{t},\boldsymbol{\lambda},\boldsymbol{\eta}}) \subseteq \mathbb{F}_{q^m}^n \ .$$

Since $\mathcal{V}_{k,\boldsymbol{t},\boldsymbol{\lambda},\boldsymbol{\eta}}$ is an $\mathbb{F}_{q^m}$-linear subspace of $\mathbb{F}_{q^m}[x;\sigma]_{<n}$ and $\mathrm{ev}_{\boldsymbol{\alpha}}(\cdot)$ is an injective linear map on $\mathbb{F}_{q^m}[x;\sigma]_{<n}$, a twisted Gabidulin code is an $\mathbb{F}_{q^m}$-linear code of length n and dimension k.

Note that given λ_i, there are unique constants $\lambda_{i,0}, \ldots, \lambda_{i,k-1} \in \mathbb{F}_{q^m}$, not all zero, and such that $\lambda_i(f_0, \ldots, f_{k-1}) = \lambda_{i,0} f_0 + \ldots + \lambda_{i,k-1} f_{k-1}$. We will call the $\lambda_{i,j}$ the *coefficients* of λ_i. In the sequel, whenever we introduce $\boldsymbol{\lambda}$, then we take $\lambda_{i,j}$ to be the coefficients of the entries of $\boldsymbol{\lambda}$.

4 Twisted Gabidulin Codes that are MRD

Not all twisted Gabidulin codes as defined in the preceding section will be MRD. In this section, we first give a linear-algebraic condition for when this will be the case, and we then use this to describe an explicit family of twisted Gabidulin codes which are MRD.

Lemma 1. *Let $n, k, \boldsymbol{t}, \boldsymbol{\lambda}, \boldsymbol{\eta}$ be chosen as in Section 3.2. For any $\mathcal{S} \subset \langle \alpha_1, \ldots, \alpha_n \rangle_{\mathbb{F}_q}$ with $\dim_{\mathbb{F}_q} \mathcal{S} = k$, consider the homogeneous, linear system of equations in the $g_0, \ldots, g_{t_\ell - 1}$:*

$$\sum_{j=0}^{t_\ell - 1} g_j T_{i,j}^{(\mathcal{S})} = 0 \quad \text{for } i = k, \ldots, k - 1 + t_\ell \ , \tag{1}$$

where

$$T_{i,j}^{(\mathcal{S})} = \begin{cases} \eta_\kappa^{-1} \sigma^j(a_{i-j}) - \sum_{\mu=0}^{k-1} \lambda_{\kappa,\mu} \sigma^j(a_{\mu-j}) & \text{if } i = k - 1 + t_\kappa \text{ for } \kappa \in \{1, \ldots, \ell\} \\ \sigma^j(a_{i-j}) & \text{otherwise} \end{cases} ,$$

and $\sum_{i=0}^{k} a_i x^i := \mathcal{A}_{\mathcal{S}}(x)$ *and* $a_i := 0$ *for* $i < 0$ *or* $i \geq k$. *The twisted Gabidulin code* $\mathcal{C}_k(\boldsymbol{\alpha}, \boldsymbol{t}, \boldsymbol{\lambda}, \boldsymbol{\eta})$ *is MRD if and only if there is no choice of* $\mathcal{S}$ *admitting a non-zero solution to the linear system.*

Proof. Let $f \in \mathcal{V}_{k,\boldsymbol{t},\boldsymbol{\lambda},\boldsymbol{\eta}}$ be a polynomial whose root space intersects with $\langle \alpha_1, \ldots, \alpha_n \rangle$ in at least k dimensions, i.e.,

$$\dim\left(\ker(f) \cap \langle \alpha_1, \ldots, \alpha_n \rangle\right) \geq k.$$

This means that there is a k-dimensional subspace $\mathcal{S} \subseteq \langle \alpha_1, \ldots, \alpha_n \rangle$ such that the annihilator polynomial $\mathcal{A}_{\mathcal{S}}$ divides f from the right, i.e. $f = g \cdot \mathcal{A}_{\mathcal{S}}$ for some $g \in \mathbb{F}_{q^m}[x;\sigma]$. Write $g = \sum_{i=0}^{t_\ell - 1} g_i x^i$ and $\mathcal{A}_{\mathcal{S}} = \sum_{i=0}^{k} a_i x^i$, as well as $a_i := 0$ for $i < 0$ or $i \geq k$. Then the i-th coefficient of f is given by

$$f_i = \sum_{j=0}^{t_\ell - 1} g_j \sigma^j\left(a_{i-j}\right) \ .$$

On the other hand, for $i \geq k$, then f_i also satisfies

$$f_i = \begin{cases} \eta_\kappa \lambda_\kappa(f_0, \ldots, f_{k-1}) & \text{if } i = k - 1 + t_\kappa \text{ for } \kappa \in \{1, \ldots, \ell\}, \\ 0 & \text{otherwise .} \end{cases}$$

For the case $i = k - 1 + t_\kappa$, combining and rewriting yields

$$0 = \sum_{j=0}^{t_\ell - 1} g_j \cdot \left(\eta_\kappa^{-1} \sigma^j\left(a_{i-j}\right) - \sum_{\mu=0}^{k-1} \lambda_{\kappa,\mu} \sigma^j\left(a_{\mu-j}\right) \right).$$

Thus, for a given $\mathcal{S}$, a non-zero solution of the linear system (1) corresponds to a non-zero polynomial $f = g \cdot \mathcal{A}_{\mathcal{S}} \in \mathcal{V}_{k,\boldsymbol{t},\boldsymbol{\lambda},\boldsymbol{\eta}}$ with

$$\mathrm{rk}(\mathrm{ev}_{\boldsymbol{\alpha}}(f)) = n - \dim\left(\ker(f) \cap \langle \alpha_1, \ldots, \alpha_n \rangle\right) \leq n - k.$$

The code $\mathcal{C}_k(\boldsymbol{\alpha}, \boldsymbol{t}, \boldsymbol{\lambda}, \boldsymbol{\eta})$ is MRD if and only if all non-zero $f \in \mathcal{V}_{k,\boldsymbol{t},\boldsymbol{\lambda},\boldsymbol{\eta}}$ result in codewords of rank $\geq n - k + 1$, which is true if and only if the system (1) has no non-zero solution for any subspace $\mathcal{S}$. □

For a given subspace $\mathcal{S}$, the system (1) is of the form

$$\underbrace{\begin{bmatrix} \eta_{t_\ell}^{-1} + \square & \square & \cdots & \square & \square & \square & \cdots & \square & \square & \cdots \\ \square & 1 & & & & & & & & \\ \vdots & \vdots & \ddots & & & & & & & \\ \square & \square & \cdots & 1 & & & & & & \\ \eta_{t_{\ell-1}}^{-1} \square + \square & \eta_{t_{\ell-1}}^{-1} \square + \square & \cdots & \eta_{t_{\ell-1}}^{-1} \square + \square & \eta_{t_{\ell-1}}^{-1} + \square & \square & \cdots & \square & \square & \cdots \\ \square & \square & \cdots & \square & \square & 1 & & & & \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & & & \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & & & \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & & & \\ \square & \square & \cdots & \square & \square & \square & \cdots & 1 & & \\ \eta_{t_1}^{-1} \square + \square & \eta_{t_1}^{-1} \square + \square & \cdots & \eta_{t_1}^{-1} \square + \square & \eta_{t_1}^{-1} \square + \square & \eta_{t_1}^{-1} \square + \square & \cdots & \eta_{t_1}^{-1} \square + \square & \eta_{t_1}^{-1} + \square & \cdots \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots \end{bmatrix}}_{=: \boldsymbol{B}_{\mathcal{S}}} \begin{bmatrix} g_{t_\ell} \\ g_{t_\ell - 1} \\ \vdots \\ g_1 \\ g_0 \end{bmatrix} = \mathbf{0}, \tag{2}$$

where the boxes $\square$ represent elements in the $\mathbb{F}_q$-span of the $\lambda_{i,j}$, $\alpha_1, \ldots, \alpha_n$, and their q-powers. The diagonal elements are either 1 (if the row corresponds to an index i with $i \neq k-1+t_\kappa$ for all κ) or $\eta_{t_\kappa}^{-1} + \square$ (if $i \neq k-1+t_\kappa$) due to $\sigma^{i-k}(a_{i-(i-k)}) = \sigma^{i-k}(a_k) = 1$ for all $i = k, k+1, \ldots, k-1+t_\ell$ (note that the diagonal elements are the $T_{i,j}^{(\mathcal{S})}$ of Equation (1) with $j = i-k$). Also, all elements above the diagonal do not depend on the $\eta_{t_\kappa}^{-1}$ since $a_{i-j} = 0$ for all $i > j+k$.

Using Lemma 1, we can give the following sufficient condition for a twisted Gabidulin code to be MRD.

Theorem 1. *Let $s_0, \ldots, s_\ell \in \mathbb{N}$ such that $\mathbb{F}_q \subseteq \mathbb{F}_{q^{s_0}} \subsetneq \mathbb{F}_{q^{s_1}} \subsetneq \cdots \subsetneq \mathbb{F}_{q^{s_\ell}} = \mathbb{F}_q$ is a chain of subfields. Let $k < n \leq s_0$ and $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_{q^{s_0}}$ be linearly independent over $\mathbb{F}_q$, and let $\boldsymbol{t}$, $\boldsymbol{\lambda}$, and $\boldsymbol{\eta}$ be chosen as in Section 3.2 with the additional requirements $\eta_i \in \mathbb{F}_{q^{s_i}} \setminus \mathbb{F}_{q^{s_{i-1}}}$ and $\lambda_{i,j} \in \mathbb{F}_{q^{s_0}}$ for all i, j. Then, the twisted Gabidulin code $\mathcal{C}_k(\boldsymbol{\alpha}, \boldsymbol{t}, \boldsymbol{\lambda}, \boldsymbol{\eta})$ is MRD.*

Proof. We prove the claim using Lemma 1. Let $\mathcal{S} \subseteq \langle \alpha_1, \ldots, \alpha_n \rangle$ be a k-dimensional subspace. We show that the system (1) has no non-zero solution. Since $\lambda_{i,j} \in \mathbb{F}_{q^{s_0}}$, $a_i \in \langle \alpha_1, \ldots, \alpha_n \rangle \subseteq \mathbb{F}_{q^{s_0}}$, $\sigma(\mathbb{F}_{q^{s_0}}) = \mathbb{F}_{q^{s_0}}$, the boxes $\square$ of the system's matrix $\boldsymbol{B}_{\mathcal{S}}$ as in (2) represent elements from $\mathbb{F}_{q^{s_0}}$.

We now consider the $\eta_{t_\kappa}^{-1}$'s to be indeterminates. This means that $\det(\boldsymbol{B}_{\mathcal{S}}) \in \mathbb{F}_{q^{s_0}}[\eta_{t_1}^{-1}, \ldots, \eta_{t_\ell}^{-1}]$ is a multivariate polynomial, where each indeterminate $\eta_{t_\kappa}^{-1}$ appears at most of degree 1 in each monomial. Let $\boldsymbol{B}_{\mathcal{S}}^{(\mu)}$ be the $(\mu \times \mu)$-bottom-right submatrix of $\boldsymbol{B}_{\mathcal{S}}$. We distinguish two cases:

(i) If $\mu \neq t_\kappa$ for all κ, then the first row of $\boldsymbol{B}_{\mathcal{S}}^{(\mu)}$ is of the form $[1, 0, \ldots, 0]$ and by Laplace's rule we get

$$\det\left(\boldsymbol{B}_{\mathcal{S}}^{(\mu)}\right) = \det\left(\boldsymbol{B}_{\mathcal{S}}^{(\mu-1)}\right).$$

(ii) If $\mu = t_\kappa$ for some κ, then $\boldsymbol{B}_{\mathcal{S}}^{(\mu)}$ contains only $\eta_{t_1}^{-1}, \ldots, \eta_{t_{\kappa-1}}^{-1}$ in its rows 2 to μ and since the first row is of the form $[\eta_{t_\kappa}^{-1} + \square, \square, \ldots, \square]$, the determinant fulfills

$$\det\left(\boldsymbol{B}_{\mathcal{S}}^{(\mu)}\right) = (\eta_{t_\kappa}^{-1} + T_\mu) \cdot \det\left(\boldsymbol{B}_{\mathcal{S}}^{(\mu-1)}\right) + U_\mu \in \mathbb{F}_{q^{s_0}}[\eta_{t_1}^{-1}, \ldots, \eta_{t_\kappa}^{-1}],$$

where $T_\mu \in \mathbb{F}_{q^{s_0}}$ and $U_\mu \in \mathbb{F}_{q^{s_0}}[\eta_{t_1}^{-1}, \ldots, \eta_{t_{\kappa-1}}^{-1}]$.

Combined, we get $\det(\boldsymbol{B}_{\mathcal{S}}^{(t_\kappa)}) = (\eta_{t_\kappa}^{-1} + T_{t_\kappa}) \det(\boldsymbol{B}_{\mathcal{S}}^{(t_{\kappa-1})}) + U_{t_\kappa} \in \mathbb{F}_{q^{s_0}}[\eta_{t_1}^{-1}, \ldots, \eta_{t_\kappa}^{-1}]$, where $\det(\boldsymbol{B}_{\mathcal{S}}^{(t_1)}) = \eta_{t_1}^{-1}$, and by recursively substituting $\eta_\kappa \in \mathbb{F}_{q^{s_\kappa}} \setminus \mathbb{F}_{q^{s_{\kappa-1}}}$ for $\kappa = 1, \ldots, \ell$, we obtain

$$\det\left(\boldsymbol{B}_{\mathcal{S}}^{(t_\kappa)}\right) \in \mathbb{F}_{q^{s_\kappa}} \setminus \{0\},$$

since $\eta_{t_\kappa}^{-1} \in \mathbb{F}_{q^{s_\kappa}} \setminus \mathbb{F}_{q^{s_{\kappa-i}}}$, $\det(\boldsymbol{B}_{\mathcal{S}}^{(t_{\kappa-1})}) \in \mathbb{F}_{q^{s_{\kappa-1}}} \setminus \{0\}$, and $U_{t_\kappa} \in \mathbb{F}_{q^{s_{\kappa-1}}}$. Hence, also $\det(\boldsymbol{B}_{\mathcal{S}}) = \det(\boldsymbol{B}_{\mathcal{S}}^{(t_\ell)}) \neq 0$ and System (1) has only the zero solution. $\square$

Theorem 1 provides a tool to systematically construct MRD twisted Gabidulin codes. For some m, we can obtain codes of length up to $2^{-\ell}m$ in this way:

Corollary 1. *Let $\ell \in \mathbb{Z}_{>0}$ and $2^\ell \mid m$. Then there is an ℓ-twisted MRD code of length $n = 2^{-\ell}m$ over $\mathbb{F}_{q^m}$.*

5 Non-Equivalence to Other MRD Codes

In this section, we show that the new family of twisted Gabidulin codes contains codes that are neither equivalent to a generalised Gabidulin nor to the twisted Gabidulin codes constructed in [23]. We use the following notion for equivalence of linear rank-metric codes.

Definition 4 ([16]). *Two linear rank-metric codes $\mathcal{C}, \mathcal{C}' \subseteq \mathbb{F}_{q^m}^n$ are (semi-linearly) equivalent if there are $\lambda \in \mathbb{F}_{q^m}^*$, $\boldsymbol{A} \in \mathrm{GL}_n(q)$, and $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ such that*

$$\mathcal{C}' = \sigma(\lambda\mathcal{C})\boldsymbol{A},$$

where $\sigma(\lambda\mathcal{C})\boldsymbol{A} := \{[\sigma(\lambda c_1), \ldots, \sigma(\lambda c_n)] \cdot \boldsymbol{A} : [c_1, \ldots, c_n] \in \mathcal{C}\}$.

Since for twisted Gabidulin codes, we can only guarantee them to be MRD for $n < m$, we cannot directly rely on the tools developed in [23] for proving the inequivalence to Gabidulin codes. We first need to state two lemmas.

Lemma 2. *Suppose $\boldsymbol{\alpha} = [\alpha_1, \cdots, \alpha_n]$ is a list of elements of $\mathbb{F}_{q^m}$, linearly independent over $\mathbb{F}_q$, and $f, g \in \mathbb{F}_{q^n}[x, \sigma]$, with $\deg(f), \deg(g) < m$. Then*

$$\mathrm{ev}_{\boldsymbol{\alpha}}(f) = \mathrm{ev}_{\boldsymbol{\alpha}}(g) \Leftrightarrow f - g \equiv 0 \mod_{\mathrm{r}} \mathcal{A}_{\boldsymbol{\alpha}}$$

Lemma 3. *Suppose $\mathcal{V}, \mathcal{V}'$ are two $\mathbb{F}_{q^m}$-subspaces of $\mathbb{F}_{q^m}[x, \sigma]$, and $\boldsymbol{\alpha}, \boldsymbol{\beta}$ two lists of n elements of $\mathbb{F}_{q^m}$, each linearly independent over $\mathbb{F}_q$. Then $\mathrm{ev}_{\boldsymbol{\alpha}}(\mathcal{V})$ is semi-linearly equivalent to $\mathrm{ev}_{\boldsymbol{\beta}}(\mathcal{V}')$ if and only if there exist elements $\psi, \phi \in \mathbb{F}_{q^m}[x, \sigma]$ such that ψ is a monomial, $\mathrm{gcrd}(\phi, x^m - 1) = 1$, and*

$$\{f \mod_{\mathrm{r}} \mathcal{A}_{\boldsymbol{\alpha}} : f \in \mathcal{V}\} = \{\psi g \phi \mod_{\mathrm{r}} \mathcal{A}_{\boldsymbol{\alpha}} : g \in \mathcal{V}'\}.$$

Furthermore, if $\mathrm{ev}_{\boldsymbol{\alpha}}(\mathcal{V})$ is equivalent to $\mathrm{ev}_{\boldsymbol{\beta}}(\mathcal{V}')$ then there exist $\psi, \phi \in \mathbb{F}_{q^m}[x, \sigma]$ such that ψ is monomial, $\deg(\phi') < n$, $\mathrm{gcrd}(\phi', \mathcal{A}_{\boldsymbol{\alpha}}) = 1$, and

$$\{f \mod_{\mathrm{r}} \mathcal{A}_{\boldsymbol{\alpha}} : f \in \mathcal{V}\} = \{\psi g \phi' \mod_{\mathrm{r}} \mathcal{A}_{\boldsymbol{\alpha}} : g \in \mathcal{V}'\}.$$

Proof. Suppose $\mathrm{ev}_{\boldsymbol{\alpha}}(\mathcal{V}) = \sigma^i(\lambda\,\mathrm{ev}_{\boldsymbol{\beta}}(\mathcal{V}'))\mathbf{A}$. Let $\psi = \lambda^{\sigma^\ell} x^\ell$, and let ϕ be such that $\phi(\alpha_i) = \sum_j A_{ji}\beta_j$, where the A_{ji}'s are the entries of $\mathbf{A}$. As $\mathbf{A}$ is invertible, and as $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ are linearly independent, ϕ can be chosen so that it does not evaluate to zero on any element of $\mathbb{F}_{q^m}^*$; in other words, $\mathrm{gcrd}(\phi, x^m - 1) = 1$. Now

$$\begin{aligned}\sigma^\ell(\lambda\,\mathrm{ev}_{\boldsymbol{\beta}}(g))\mathbf{A} &= \left(\lambda^{\sigma^\ell}(x^\ell g)\left(\sum_j A_{j1}\beta_j\right), \ldots, \lambda^{\sigma^\ell}(x^\ell g)\left(\sum_j A_{jn}\beta_n\right)\right) \\ &= (\lambda^{\sigma^\ell}(x^\ell g)(\phi(\alpha_1)), \ldots, \lambda^{\sigma^\ell}(x^\ell g)(\phi(\alpha_1)) = \mathrm{ev}_\alpha(\psi g \phi),\end{aligned}$$

and so

$$\{\mathrm{ev}_{\boldsymbol{\alpha}}(f) : f \in \mathcal{V}\} = \{\mathrm{ev}_{\boldsymbol{\beta}}(g) : g \in \mathcal{V}'\} = \{\mathrm{ev}_{\boldsymbol{\alpha}}(\psi g \phi) : g \in \mathcal{V}'\},$$

so taking this together with Lemma 2 gives the first result.

For the second part, we take ϕ' to be the remainder of ϕ on right division by $\mathcal{A}_{\boldsymbol{\alpha}}$, i.e. $\phi = a\mathcal{A}_{\boldsymbol{\alpha}} + \phi'$, with $\deg(\phi') < \deg(\mathcal{A}_{\boldsymbol{\alpha}}) = n$. Then the result follows immediately. □

In the following, we consider the special case of twisted Gabidulin codes, given by evaluation polynomials of the form

$$\mathcal{V}_{k,t,\eta} := \left\{ \sum_{i=0}^{k-1} f_i x^i + \eta f_0 x^{k-1+t} : f_i \in \mathbb{F}_{q^m} \right\}. \tag{3}$$

Note that these are contained in the codes constructed in [23] precisely when $t = 1$, and with Gabidulin codes precisely when $\eta = 0$. The following theorem proves that any twisted Gabidulin code $\mathrm{ev}_{\boldsymbol{\alpha}}(\mathcal{V}_{k,t,\eta})$ with $1 < t < s-1$ and $\eta \neq 0$ is not equivalent to one of these code classes. Since generalised Gabidulin codes are equivalent to Gabidulin codes (cf. [11]), such twisted Gabidulin codes are also not equivalent to one of them.

Theorem 2. *Let $\boldsymbol{\alpha}$ be an $\mathbb{F}_q$-basis for $\mathbb{F}_{q^s} \leq \mathbb{F}_{q^m}$. Let $1 < t < s-1$ and $\eta \neq 0$. Then the code $\mathrm{ev}_{\boldsymbol{\alpha}}(\mathcal{V}_{k,t,\eta})$ is not equivalent to $\mathrm{ev}_{\boldsymbol{\beta}}(\mathcal{V}_{k,1,\eta'})$ for any $\boldsymbol{\beta}, \eta'$.*

Proof. We have that $\mathcal{A}_{\boldsymbol{\alpha}} = x^s - 1$. As $x^i \in \mathcal{V}_{k,1,\eta'}$ for $i \in \{1, \ldots, k-1\}$, by Lemma 3 we must have

$$\psi x^i \phi \mod_{\mathrm{r}} (x^s - 1) \in \mathcal{V}_{k,t,\eta}$$

Let $\psi = x^\ell$ and $\phi = \sum_{j=0}^{s-1} \phi_j x^j$. Note that $x^\ell \mathcal{V}_{k,t,\eta} x^{s-\ell} = \mathcal{V}_{k,t,\eta}$, and $x^\ell \mathcal{V}_{k,1,\eta'} x^{s-\ell} = \mathcal{V}_{k,1,\eta'}$, and so without loss of generality we may assume that $\ell = 0$. Hence we have

$$\sum_j \phi_j^{\sigma^i} x^{i+j} \mod s \in \mathcal{V}_{k,t,\eta}$$

for all $i \in \{1, \ldots, k-1\}$. As the coefficient of x^r is zero for every element of $\mathcal{V}_{k,t,\eta}$ for $r \notin \{0, \ldots, k-1\} \cup \{k+t-1\}$, we must have that $\phi_j = 0$ whenever $i + j \notin \{0, \ldots, k-1\} \cup \{k+t-1\}$. Hence we get that $\phi = \phi_0 + \phi_{s-1} x^{s-1}$.

If $\eta' = 0$, then as $1 \in \mathcal{V}_{k,1,\eta'}$ we get that $\phi_0 + \phi_{s-1} x^{s-1} \in \mathcal{V}_{k,t,\eta}$, which implies $\phi = 0$, a contradiction. Suppose now that $\eta' \neq 0$. Then as $1 + \eta' x^k \in \mathcal{V}_{k,1,\eta'}$, we get that

$$(1 + \eta' x^k)(\phi_0 + \phi_{s-1} x^{s-1}) \mod_{\mathrm{r}} (x^s - 1) \in \mathcal{V}_{k,t,\eta}.$$

But this is equal to

$$\phi_0 + \phi_{s-1} x^{s-1} + \eta' \phi_0^{\sigma^k} x^k + \eta' \phi_{s-1} x^{k-1},$$

and so as $t > 1$ the coefficient of x^k must be zeros, implying $\phi_0 = 0$, and as $s - 1 > k + t$ we must have $\phi_{s-1} = 0$, implying $\phi = 0$, a contradiction. □

6 Possible Application

The rank-metric variant GPT [8] of the McEliece public-key cryptosystem [15] was a potential candidate to reduce the size of the public key until structural attacks on the system were found [9, 10]. Since then, many variants of GPT have been proposed and broken, see [20] for an overview.

Structural attacks on a variant of the McEliece cryptosystem based on the twisted Gabidulin codes in [23] can be efficiently performed since any such code of dimension k is a subcode of a Gabidulin code of dimension $k + 1$. Such an immediate attack is not possible for the new twisted Gabidulin codes since such a code is only subcode of a $(k - 1 + t_\ell)$-dimensional Gabidulin code, which does not help the attacker if t_ℓ is sufficiently large.

Therefore, twisted Gabidulin codes should be thorougly analysed for their suitability in the McEliece cryptosystem. An immediate necessity is the existence of an efficient decoding algorithm, but also possibilities for structural attacks should be investigated.

7 Conclusion

We introduced a new constructive class of rank-metric codes, twisted Gabidulin codes, that contain codes inequivalent to existing classes, such as Gabidulin or the twisted Gabidulin codes in [23]. It was proved that MRD twisted Gabidulin codes exist for n up to $2^{-\ell}m$. Similar to the results on twisted Reed–Solomon codes [2], longer codes might be possible.

References

1. Augot, D., Loidreau, P., Robert, G.: Rank Metric and Gabidulin Codes in Characteristic Zero. In: IEEE ISIT. pp. 509–513 (2013)
2. Beelen, P., Puchinger, S., Rosenkilde né Nielsen, J.: Twisted Reed–Solomon Codes. In: IEEE ISIT (2017)
3. Boucher, D., Ulmer, F.: Linear Codes using Skew Polynomials with Automorphisms and Derivations. Designs, Codes and Cryptography 70(3), 405–431 (2014)
4. Cossidente, A., Marino, G., Pavese, F.: Non-Linear Maximum Rank Distance Codes. Designs, Codes and Cryptography 79(3), 597–609 (2016)
5. Delsarte, P.: Bilinear Forms over a Finite Field with Applications to Coding Theory. J. Combin. Theory Ser. A 25(3), 226–241 (1978)
6. Gabidulin, E.M.: Theory of Codes with Maximum Rank Distance. Probl. Inf. Transm. 21(1), 3–16 (1985)
7. Gabidulin, E.M., Bossert, M., Lusina, P.: Space-Time Codes Based on Rank Codes. In: IEEE ISIT. p. 284 (2000)
8. Gabidulin, E.M., Paramonov, A., Tretjakov, O.: Ideals Over a Non-Commutative Ring and Their Application in Cryptology. In: Workshop on the Theory and Application of of Cryptographic Techniques. pp. 482–489. Springer (1991)
9. Gibson, J.: Severely Denting the Gabidulin Version of the McEliece Public Key Cryptosystem. Designs, Codes and Cryptography 6(1), 37–45 (1995)

10. Gibson, K.: The Security of the Gabidulin Public Key Cryptosystem. In: International Conference on the Theory and Applications of Cryptographic Techniques. pp. 212–223. Springer (1996)
11. Horlemann-Trautmann, A.L., Marshall, K.: New Criteria for MRD and Gabidulin Codes and Some Rank-Metric Code Constructions. arXiv preprint arXiv:1507.08641 (2015)
12. Kshevetskiy, A., Gabidulin, E.: The New Construction of Rank Codes. In: IEEE ISIT. pp. 2105–2108 (2005)
13. Lunardon, G., Trombetti, R., Zhou, Y.: Generalized twisted Gabidulin codes. arXiv preprint arXiv:1507.07855 (2015)
14. McDonald, B.R.: Finite Rings With Identity, vol. 28. Marcel Dekker Incorporated (1974)
15. McEliece, R.J.: A Public-Key Cryptosystem Based on Algebraic Coding Theory. Coding Thv 4244, 114–116 (1978)
16. Morrison, K.: Equivalence for Rank-Metric and Matrix Codes and Automorphism Groups of Gabidulin codes. IEEE Trans. Inf. Theory 60(11), 7035–7046 (2014)
17. Ore, O.: Theory of Non-Commutative Polynomials. Ann. Math. 34(3), 480–508 (Jul 1933)
18. Otal, K., Özbudak, F.: Explicit Construction of Some Non-Gabidulin Linear Maximum Rank Distance Codes. Advances in Mathematics of Communications 10(3) (2016)
19. Otal, K., Özbudak, F.: Additive rank metric codes. IEEE Trans. Inf. Theory 63(1), 164–168 (2017)
20. Overbeck, R.: Structural Attacks for Public Key Cryptosystems Based on Gabidulin Codes. Journal of Cryptology 21(2), 280–301 (2008)
21. Roth, R.M.: Maximum-Rank Array Codes and their Application to Crisscross Error Correction. IEEE Trans. Inf. Theory 37(2), 328–336 (1991)
22. Roth, R.M.: Tensor Codes for the Rank Metric. IEEE Trans. Inf. Theory 42(6), 2146–2157 (1996)
23. Sheekey, J.: A New Family of Linear Maximum Rank Distance Codes. Advances in Mathematics of Communications pp. 475–488 (2016)
24. Silberstein, N., Rawat, A.S., Vishwanath, S.: Error Resilience in Distributed Storage via Rank-Metric Codes. In: 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton). pp. 1150–1157. IEEE (2012)
25. Silva, D., Kschischang, F.R., Koetter, R.: A Rank-Metric Approach to Error Control in Random Network Coding. IEEE Trans. Inf. Theory 54(9), 3951–3967 (2008)